

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

---

In re Patent Application of:  
Richard S. Slevin

Application No.: 09/761,112

Confirmation No.: 3637

Filed: January 16, 2001

Art Unit: 2131

---

For: Access control apparatus and method for  
electronic device

Examiner: S. Zia

**AMENDMENT IN RESPONSE TO NOTICE OF NON-COMPLIANT AMENDMENT**

MS Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

**INTRODUCTORY COMMENTS**

In response to the Notice of Non-Compliant Amendment dated April 12, 2005,  
please amend the above-identified U.S. patent application as follows:

**Amendments to the Claims** are reflected in the listing of claims which begins  
on page 2 of this paper.

**Remarks/Arguments** begin on page 12 of this paper.

**AMENDMENTS TO THE CLAIMS**

Claim 1 (Previously presented): A biometric-controlled power gate controlling a power flow from a power source to an electrically powered device, comprising:

- a circuit of the device energized by the power flow for enabling a startup procedure of a processor of the device;
- a biometric-controlled switch, coupled to said circuit between the power source and said processor, for enabling said energizing of said circuit responsive to an assertion of a biometric activation signal; and
- a biometric reader coupled to said biometric-controlled switch, comprising:
  - a memory for storing a biometric signature;
  - a biometric sensor, coupled to said memory, for discerning a biometric profile; and
  - a verifier, coupled to said biometric sensor and to said memory, for asserting said biometric activation signal when said biometric profile matches said biometric signature wherein the device is inoperable from the power source until said assertion of said biometric activation signal.

Claim 2 (Previously presented): A method for power gating an electronic device powered from a power source, comprising:

- discerning a biometric profile of a prospective user of the electronic device; and
- comparing said biometric profile to a stored biometric signature of an authorized user of the electronic device; and thereafter asserting a biometric activation signal to a biometric-controlled switch when said prospective user is an authorized user, said biometric-controlled switch interposed between the power source and a circuit of

the electronic device for enabling a startup procedure of said electronic device such that said biometric-controlled switch interrupts power to said circuit when said activation signal is not asserted wherein the startup procedure is inoperable from the power source until said assertion of said biometric activation signal.

Claim 3 (Previously presented): A biometric power gating system for controlling power from a power source to a circuit, comprising: an electronic device including the circuit operable from the power provided from the power source; a biometric-controlled switch, coupled to said electronic device between the power source and the circuit, for gating the power from the power source responsive to a biometric activation signal; and a biometric reader for asserting said biometric activation signal responsive to a verification of a user biometric signature wherein said electronic device is inoperable from the power from the power source until said biometric activation signal is asserted.

Claim 4 (Previously presented): The biometric system of claim 3 wherein said biometric signature includes a fingerprint.

Claim 5 (Previously presented): The biometric system of claim 3 wherein said biometric signature includes a retinal pattern.

Claim 6 (Previously presented): The biometric system of claim 3 wherein said electronic device includes a portable electronic device.

Claim 7 (Previously presented): The biometric system of claim 6 wherein said portable electronic device includes a personal data assistant (PDA).

Claim 8 (Previously presented): The biometric system of claim 6 wherein said portable electronic device includes a laptop computer.

Claim 9 (previously presented): The biometric system of claim 3 wherein the power source includes a battery.

Claim 10 (Previously presented): The biometric system of claim 3 wherein the power source includes a power supply.

Claim 11 (Previously presented): The biometric system of claim 3 wherein the power source includes a direct power supply.

Claim 12 (Previously presented): The biometric system of claim 3 wherein said switch is integrated into said electronic device.

Claim 13 (Previously presented): The biometric system of claim 3 wherein said switch is integrated into the power source.

Claim 14 (Previously presented): The biometric system of claim 3 wherein said switch is integrated into said biometric reader.

Claim 15 (Previously presented): The biometric system of claim 3 wherein said switch is a state device for storing an operational mode.

Claim 16 (Previously presented): The biometric system of claim 15 wherein said operational mode maintains said gating of said power from the power source after receiving an asserted activation signal.

Claim 17 (Previously presented): The biometric system of claim 16 wherein said operational mode is reset to disable the power from the power source when said electronic device is inactivated pending reassertion of said activation signal.

Claim 18 (Previously presented): The biometric system of claim 3 wherein said electronic device includes a plurality of BIOS routines and

wherein said switch selectively activates one or more of said BIOS routines responsive to said activation signal.

Claim 19 (Previously presented): The biometric system of claim 18 wherein said biometric reader discriminates between a first user and a second user, with said activation signal identifying a particular one of said users.

Claim 20 (Previously presented): The biometric system of claim 19 wherein said switch selectively activates said one or more said BIOS routine responsive to said particular one user with said switch activating a different one or more of said BIOS routines for said first user than activated for said second user.

Claim 21 (Previously presented): The biometric system of claim 3 wherein said electronic device enables access to a set of resources responsive to an authentication and wherein said switch provides said authentication responsive to said activation signal.

Claim 22 (Previously presented): The biometric system of claim 21 wherein said biometric reader discriminates between a first user and a second user, with said activation signal identifies a particular one of said users.

Claim 23 (Previously presented): The biometric system of claim 22 wherein said switch selectively enables access to one or more resources of said set of resources responsive to said particular one user with said switch signaling enablement of a different one or more resources for said first user than enabled for said second user.

Claim 24 (Previously presented): A biometric-mediated power gating method, comprising:

- a) establishing a biometric profile from a prospective user;
- b) comparing said biometric profile to a biometric signature;
- c) asserting a biometric activation signal when said profile and said signature match; and
- d) gating, responsive to said biometric activation signal, power from a power source to an electronic device using a biometric switch coupled to said biometric activation signal to enable operation of said electronic device wherein said electronic device is inoperable from said power source until said assertion of said biometric activation signal and wherein said biometric access control is disposed between said power source and said electronic device to control said power therethrough.

Claim 25 (Previously presented): The method of claim of 24 wherein said gating step d) operation enablement includes initiating a boot sequence of said electronic device.

Claim 26 (Previously presented): A biometric-mediated power gating method, comprising:

- a) asserting a biometric activation signal responsive to a verification of a user biometric signature; and
- b) gating, responsive to said biometric activation signal, power from a power source to an electronic device operable from said power using a biometric-controlled switch operably disposed between said power source and said electronic device wherein said electronic device is inoperable from said power source until said assertion of said biometric activation signal.

Claim 27 (Previously presented): The biometric-mediated power gating method of claim 26 wherein said biometric signature includes a fingerprint.

Claim 28 (Previously presented): The biometric-mediated power gating method of claim 26 wherein said biometric signature includes a retinal pattern.

Claim 29 (Previously presented): The biometric-mediated power gating method of claim 26 wherein said electronic device includes portable electronic device.

Claim 30 (Previously presented): The biometric-mediated power gating method of claim 29 wherein said portable electronic device includes a personal data assistant (PDA).

Claim 31 (Previously presented): The biometric-mediated power gating method of claim 29 wherein said portable electronic device includes a laptop computer.

Claim 32 (Previously presented): The biometric-mediated power gating method of claim 26 wherein said power source includes a battery.

Claim 33 (Previously presented): The biometric-mediated power gating method of claim 26 wherein said power source includes a power supply.

Claim 34 (Previously presented): The biometric-mediated power gating method of claim 26 wherein said power source includes a direct power.

Claim 35 (Previously presented): The biometric-mediated power gating method of claim 26 wherein said switch is integrated into said electronic device.

Claim 36 (Previously presented): The biometric-mediated power gating method of claim 26 wherein said switch is integrated into said power source.

Claim 37 (Previously presented): The biometric-mediated power gating method of claim 26 wherein said switch is integrated into said biometric reader.

Claim 38 (Previously presented): The biometric-mediated power gating method of claim 26 wherein said switch is a state device for storing an operational mode.

Claim 39 (Previously presented): The biometric-mediated power gating method of claim 38 further comprising maintaining said operational mode said gating of said power from said power source after receiving an asserted activation signal.

Claim 40 (Previously presented): The biometric-mediated power gating method of claim 39 further comprising resetting said operational mode to disable said power from said power source when said electronic device is inactivated pending a reassertion of said activation signal.

Claim 41 (Previously presented): The biometric-mediated power gating method of claim 26 wherein said electronic device includes a plurality of BIOS routines, said method further comprising activating selectively one or more of said BIOS routines responsive to said activation signal.



Claim 42 (Previously presented): The biometric-mediated power gating method of claim 41 further comprising a biometric reader for asserting said activation signal responsive to said verification of said biometric signature, the method further comprising discriminating between a first user and a second user, with said activation signal identifying a particular one of said users.

Claim 43 (Previously presented): The biometric-mediated power gating method of claim 42 further comprising activating selectively said one or more said BIOS routine responsive to said particular one user wherein a different one or more of said BIOS routines are activated for said first user than are activated for said second user.

Claim 44 (Previously presented): The biometric-mediated power gating method of claim 26 wherein said electronic device enables access to a set of resources responsive to an authentication and wherein said switch provides said authentication responsive to said activation signal.

Claim 45 (Previously presented): The biometric-mediated power gating method of claim 44 further comprising discriminating between a first user and a second user, with said activation signal identifying a particular one of said users.

Claim 46 (Previously presented): The biometric-mediated power gating method of claim 45 further comprising selectively enabling access to one or more resources of said set of resources responsive to said particular one user with a different one or more resources enabled for said first user than are enabled for said second user.

Claim 47 (Previously presented): A computer program product comprising a computer readable medium carrying program instructions for power gating an electronic device when executed using a computing system, the executed program instructions executing a method, the method comprising:

- a) asserting a biometric activation signal responsive to a verification of a user biometric signature; and
- b) gating, responsive to said biometric activation signal, power from a power source to the electronic device operable from said power using a biometric-controlled switch operably disposed between said power source and the electronic device.

Claim 48 (Canceled):

Claim 49 (Previously presented): A biometric-apparatus for gating power, comprising:  
means, responsive to a verification of a user biometric signature, for asserting a biometric activation signal to enable a power source; and  
means , responsive to said biometric activation signal, for gating power from said power source to an electronic device operable from said power using a biometric-controlled switch operably disposed between said power source and said electronic device wherein said electronic device is inoperable from said power source until said assertion of said biometric activation signal.

Claim 50 (New): A biometric power gating system for controlling power from a power source to a system, comprising:  
an electronic device including the system, said electronic device operable exclusively from the power provided from the power source;  
a biometric-controlled switch, coupled to said electronic device

between the power source and the circuit, for selectively gating the power from the power source responsive to a biometric activation signal, said switch enabling the power to the system in an enabled mode and disabling all power to the system in a disabled mode; and a biometric reader for asserting said biometric activation signal responsive to a verification of a user biometric signature wherein said electronic device is inoperable from the power from the power source until said biometric activation signal is asserted.

### **REMARKS**

Upon approval of the undersigned's request for entry of the present amendment canceling claim 48 and adding new claim 50, claims 1–47 and 49–50 will be pending. Previously examined claims 1–49 were examined and claims 47–48 were rejected under 35 USC Section 101, and all pending claims were additionally rejected under 35 USC Section 103 as being unpatentable over Cromer et al. (CROMER) in view of Teitelbaum et al. (TEITELBAUM). In light of the amendments and following comments, the rejections are respectfully requested to be withdrawn.

#### *35 USC Section 101*

Canceling claim 48 moots that rejection.

Reconsideration of the rejection of claim 47 is respectfully requested. Claim 47 recites a computer program product that includes instructions for assertion of a biometricating signal and use of that signal to control power flow from a power source to an electronic device.

#### *35 USC Section 103: CROMER & TEITELBAUM*

The rejection of claims 1–47 and 49 based upon the cited references is respectfully requested to be reconsidered for at least two reasons:

a) the asserted combination fails to meet the express limitations and thus the rejection fails to present a prima facie case of obviousness; and

b) the TEITELBAUM reference is non-analogous art and thus inappropriate to combine with CROMER.

### **Prima Facie Case**

The independent claims all recite that a power gate is provided BETWEEN a power source and the electronic device/processor/circuit/system: Claim 1: "...a biometric-controlled switch, coupled to said circuit between the power source and said processor..."

Claim 2: "...said biometric-controlled switch interposed between the power source and a circuit of the electronic device for enabling a startup procedure of said electronic device..."

Claim 3: "...a biometric-controlled switch, coupled to said electronic device between the power source and the circuit..."

Claim 24 "...wherein said biometric access control is disposed between said power source and said electronic device to control said power therethrough"

Claim 47: "...using a biometric-controlled switch operably disposed between said power source and the electronic device..."

Claim 49: "...using a biometric-controlled switch operably disposed between said power source and said electronic device..."

Claim 50: "...a biometric-controlled switch, coupled to said electronic device between the power source and the circuit..."

CROMER fails to show any device between the power supply (main supply power 240 is clearly directly connected to the system components) and the "rest" of the system. The rejection fails to explain or account for this difference and thus the rejection fails to present the requisite prima facie case.

For this reason alone, all claims are respectfully asserted to be distinguished from the cited references and combination as identified in the rejection. An indication of allowability is respectfully requested.

Others of the dependent claims are independently patentable in their own right.

Specific discussion is deferred pending further examination and action on the independent claims.

*NON-ANALOGOUS ART*

The undersigned respectfully asserts that TEITELBAUM is non-analogous for at least two reasons: a) TEITELBAUM is NOT from the same field of endeavor and b) TEITELBAUM is not reasonably pertinent to the same problem solved by the present invention.

CROMER is classified in Class 713 ELECTRICAL COMPUTERS AND DIGITAL PROCESSING SYSTEMS: SUPPORT while TEITELBAUM is classified in Class 379 TELEPHONIC COMMUNICATIONS, two different classifications. While not dispositive, this is strong evidence that the two references are in different areas, with TEITELBAUM being non-analogous to the present invention as it relates to telephonic systems.

Further, TEITELBAUM deals with access restriction/permissions of a user to a telephone switch/telephonic services. There is no discussion of power supplies, gating, or the like addressed by the present invention.

In view of the above amendment, applicant believes the pending application is in condition for allowance.

Dated: July 13, 2007

Respectfully submitted,

Electronic signature: /Michael E. Woods/  
Michael E. Woods  
Registration No.: 33,466  
PATENT LAW OFFICES OF MICHAEL E.  
WOODS  
3433 Wheeling Drive  
Santa Clara, California 95051-6034  
(408) 490-4692  
(408) 490-4693 (Fax)  
Attorney For Applicant